

Few products, many h -fold sums

Albert Bush, Ernie Croot

October 21, 2014

Abstract

Improving upon a technique of Croot and Hart, we show that for every h , there exists an $\epsilon > 0$ such that if $A \subseteq \mathbb{R}$ is sufficiently large and $|A.A| \leq |A|^{1+\epsilon}$, then $|hA| \geq |A|^{\Omega(e^{\sqrt{c \log h}})}$.

1 Introduction

For a set $A \subseteq \mathbb{R}$, the sumset, product set, h -fold sumset, and h -fold product set are defined as

$$A + A := \{a + a' : a, a' \in A\},$$

$$A.A := \{a.a' : a, a' \in A\},$$

$$hA := \{a_1 + \dots + a_h : a_i \in A\},$$

$$A^{(h)} := \{a_1 \cdot \dots \cdot a_h : a_i \in A\}.$$

We prove the following theorem:

Theorem 1. *For any $h \in \mathbb{N}$, there exists an $\epsilon = \epsilon(h) > 0$ such that the following holds: there exists an $n_0 = n_0(\epsilon, h)$ such that if $A \subseteq \mathbb{R}$ is of size $n \geq n_0$ and $|A.A| \leq |A|^{1+\epsilon}$, then*

$$|hA| \geq |A|^{ce\sqrt{\frac{1}{100} \log h}}$$

for some absolute constant c .

1.1 Background

In 1983, Erdős and Szemerédi stated the following two conjectures [7]:

Conjecture 2. (*Sum-Product Problem*) *For any $\epsilon > 0$, there exists an $n_0 = n_0(\epsilon)$ such that if $A \subseteq \mathbb{R}$ is of size $n \geq n_0$, then*

$$|A.A| + |A + A| \geq |A|^{2-\epsilon}$$

Conjecture 3. (*h -fold Sum-Product Problem*) *For any $\epsilon > 0$ and for any $h \in \mathbb{N}$, there exists an n_0 such that if $A \subseteq \mathbb{R}$ is of size $n \geq n_0$, then*

$$|hA| + |A^{(h)}| \geq |A|^{h-\epsilon}$$

Although resolution of either conjecture is currently out of reach, there has been considerable progress on Conjecture 2.

Theorem 4. ([8],[9],[15],[16]) *There exists an $0 < \epsilon < 1$ and an absolute constant $c > 0$ such that for any $A \subseteq \mathbb{R}$*

$$|A + A| + |A.A| \geq c|A|^{1+\epsilon}$$

Initially, results were only proven when $A \subseteq \mathbb{Z}$. In that case Theorem 4 was first proved by Erdős and Szemerédi with an unspecified, but fixed value ϵ [7]. Their method was refined by Nathanson and then Chen who showed one could take $\epsilon = 1/31$ and $\epsilon = 1/5$ respectively [13],[4]. In the case when one assumes $A \subseteq \mathbb{R}$, Ford proved one could take $\epsilon = 1/15$. Elekes showed one could take $\epsilon = 1/4$ in \mathbb{R} by introducing a beautiful correspondence between incidence geometry and sum-product inequalities [8]. Solymosi expanded upon this connection and showed one can take $\epsilon = 3/11 - \delta$ [15], and then a few years later, $\epsilon = 1/3 - \delta$ [16] for any $\delta > 0$ given that A is sufficiently large.

Progress on Conjecture 3 has been much slower. For subsets of the integers, Bourgain and Chang showed that one can take the exponent of $|A|$ to be a function that tends to infinity along with h :

Theorem 5. [1] *For every $b > 0$, there exists and $h \in \mathbb{N}$ such that for any $A \subseteq \mathbb{Z}$*

$$|hA| + |A^{(h)}| \geq |A|^b$$

One can take b to be on the order of $(\log h)^{1/4}$. Unfortunately, there have not been any successful attempts at proving a similar result to Theorem 5 for real-valued sets. A predecessor to Theorem 5 was proved by Chang several years earlier.

Theorem 6. [2] *For any $h \in \mathbb{N}$, there exists a $K = K(h) > 0$ such that if $A \subseteq \mathbb{Z}$ and $|A.A| \leq K|A|$, then*

$$|hA| \geq c(K, h)|A|^h.$$

The restriction that $|A.A| \leq K|A|$ allowed Chang to apply Freiman's theorem to deduce strong multiplicative structure in A . However, even with the best known bounds on Freiman's theorem one cannot take K up to a power of $|A|$. Several years later, Chang showed that one can apply the Subspace Theorem to easily deduce Theorem 6 for real-valued sets [3]. In that same paper, she also proved a version of Theorem 6 that avoided the use of Freiman's theorem, but her method was restricted to integral sets. This method allows one to infer information about sets with product set equal to some power of $|A|$.

Theorem 7. [3] *For any $h \in \mathbb{N}$, there exists an $\epsilon > 0$ such that if $A \subseteq \mathbb{Z}$ and $|A.A| \leq |A|^{1+\epsilon}$, then*

$$|hA| \geq |A|^{h-\delta_h(\epsilon)}$$

where $\delta_h \rightarrow 0$ as $\epsilon \rightarrow 0$.

It would be desirable to have a version of Theorem 7 for real-valued sets. Croot and Hart were able to prove such a theorem but with a weaker conclusion.

Theorem 8. [5] *For every $h \in \mathbb{N}$ there exists an $\epsilon' := \epsilon'(h)$ such that the following holds: for any $0 < \epsilon < \epsilon'$, there exists an $n_0 := n_0(\epsilon, h)$ such that if $A \subseteq \mathbb{R}$ is of size $n \geq n_0$ and $|A.A| \leq |A|^{1+\epsilon}$, then*

$$|hA| \geq |A|^{c \log h/2 - f_h(\epsilon)}$$

where c is an absolute constant, and $f_h(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$.

Similar bounds have also been shown in unpublished papers [11] [12], but it would be desirable for many applications to have the exponent of A grow faster than logarithmically with h . Croot and Hart also proved a theorem on the h -fold sum $h(A.A)$ by introducing a method that used bounds on the Tarry-Escott problem.

Theorem 9. [5] *For every $h \in \mathbb{N}$ there exists an $\epsilon = \epsilon(h) > 0$ such that the following holds: there exists an $n_0 := n_0(\epsilon, h)$ such that if $A \subseteq \mathbb{R}$ is of size $n \geq n_0$ then*

$$|h(A.A)| \geq |A|^{\Omega((h/\log h)^{1/3})}.$$

The goal of this paper – that is, in proving Theorem 1 – is to greatly extend the techniques used in proving Theorem 9 to give a much stronger bound on hA than is found in Theorem 8.

1.2 Layout and Notation.

In Section 2, we list some well-known additive combinatorial results that we will need. We also include several lemmas that are directly from [5]. For completeness, we include the proofs of these lemmas. In Section 3 and 4, we prove new, key lemmas that we will need to prove Theorem 1. Section 5 contains the proof of Theorem 1. In addition to the notation introduced in the beginning, we define the difference and quotient set as follows:

$$A - B := \{a - b : a \in A, b \in B\}$$

$$A/B := \{a/b : a \in A, b \in B\}$$

All sets are assumed to be finite subsets of \mathbb{R} unless indicated otherwise. The additive energy $E(A, B)$ is defined as

$$\{(a, b, a', b') \in A \times B \times A \times B : a + b = a' + b'\}.$$

We say that $f \gg g$ if $g = O(f)$ and $f \gg_k g$ if $f(n) \geq c(k)g(n)$ for n sufficiently large. We say that a polynomial $p(x)$ vanishes at $x = a$ to order j if $x = a$ is a root of order j but not $j + 1$. All graphs are finite and undirected. For a graph (G, E) , $\Delta(G)$ denotes the maximum degree of G . We will abuse notation and denote $|G|$ as $|V(G)|$.

2 Lemmas and Known Results

The Plünnecke-Ruzsa inequality is ubiquitous in additive combinatorics and will be needed in our proof.

Lemma 10 (Plünnecke-Ruzsa Inequality). [14][17] *Let A be a subset of a finite abelian group such that $|A + A| \leq c|A|$. Then, $|kA - \ell A| \leq c^{k+\ell}|A|$.*

We will also need the following lemma which exists in many different forms ([17], Chap. 2).

Lemma 11. *Let $X, Y \subseteq \mathbb{R}$. Then,*

$$|X + Y| \geq \frac{|X||Y|}{|(X - X) \cap (Y - Y)|}.$$

In particular, if $(X - X) \cap (Y - Y) = \{0\}$, then $|X + Y| = |X||Y|$.

Proof. The additive energy of X and Y can be bounded from above by

$$\begin{aligned} E(X, Y) &:= |\{(x, x', y, y') \in X \times X \times Y \times Y : x + y = x' + y'\}| = |\{(x, x', y, y') : x - x' = y - y'\}| \\ &= \sum_{t \in X - X \cap Y - Y} |\{(x, x', y, y') : x - x' = t = y - y'\}| \leq |(X - X) \cap (Y - Y)| |X| |Y| \end{aligned}$$

On the other hand, one can use Cauchy-Schwarz to bound the additive energy from below:

$$E(X, Y) = \sum_{s \in X + Y} |\{(x, y) \in X \times Y : x + y = s\}|^2 \geq \frac{|X|^2 |Y|^2}{|X + Y|}.$$

Combining the two inequalities proves the lemma. \square

We will use several lemmas from [5] whose proofs we include for completeness. First, we state a result of Wooley on the Tarry-Escott problem [18].

Theorem 12. *For every $k \geq 3$, there exists two distinct sets*

$$\{a_1, \dots, a_s\}, \{b_1, \dots, b_s\} \subseteq \mathbb{Z}$$

such that for all $j = 1, \dots, k$

$$\sum_{i=1}^s a_i^j = \sum_{i=1}^s b_i^j$$

but

$$\sum_{i=1}^s a_i^{k+1} \neq \sum_{i=1}^s b_i^{k+1}.$$

Moreover, $s < (5/8)(k+1)^2$.

We will need a useful corollary of this result.

Corollary 13. *For all $k \geq 2$, there exists a monic polynomial $f(x)$ having coefficients only 0, 1, -1 having at most k^2 nonzero terms such that $f(x)$ vanishes at $x = 1$ to order exactly k .*

Proof. For $k = 2, 3$, verify the corollary by hand by considering $(x-1)(x^2-1)$ and $(x-1)(x^2-1)(x^4-1)$. For $k \geq 4$, we use Theorem 12. Note that for $k \geq 4$, we have that $k^2 \geq (5/8)(k+1)^2$. Apply Lemma 12 to get two distinct sets $\{a_1, \dots, a_s\}$ and $\{b_1, \dots, b_s\}$ with the properties stated in the lemma. If these sets are not in $\mathbb{Z}_{\geq 0}$, then let $a := \min\{a_1, \dots, a_s, b_1, \dots, b_s\}$ otherwise, $a := 0$. Let

$$f(x) := x^{-a} \sum_{i=1}^s x^{a_i} - x^{b_i}.$$

Since the sets are distinct, it is clear that the polynomial is monic, has at most k^2 nonzero terms, and only has coefficients 1, and -1 . To see that f has the correct order of vanishing at $x = 1$, we use the fact that f vanishes at $x = 1$ to order exactly k if and only if its first k derivatives vanish at $x = 1$, but the $(k+1)$ st derivative does not. Let $1 \leq \ell \leq k$. Consider the ℓ th derivative of f evaluated at $x = 1$:

$$\begin{aligned} f^{(\ell)} &= \sum_{i=1}^s (a_i - a)(a_i - 1 - a) \dots (a_i - (\ell - 1) - a) - (b_i - a)(b_i - 1 - a) \dots (b_i - (\ell - 1) - a) \\ &= \sum_{i=1}^s a_i^\ell - b_i^\ell + g_{k-1}(a_i^{\ell-1} - b_i^{\ell-1}) + \dots + g_1(a_i - b_i) + g_0 \end{aligned}$$

where g_i is some function depending on i and a . Since the a_i, b_i satisfy the conditions of Lemma 12, the ℓ th derivative is equal to zero if $1 \leq \ell \leq k$. Moreover, the $(k+1)$ st derivative of f at $x = 1$ then simplifies to

$$f^{(k+1)} = \sum_{i=1}^s a_i^{k+1} - b_i^{k+1} \neq 0.$$

So f has a zero at $x = 1$ of order precisely k . □

Lemma 14. *For every $k \in \mathbb{N}, \epsilon > 0$, there exists an $n_0 = n_0(k, \epsilon)$ such that if $A \subseteq \mathbb{R}$ is of size $n \geq n_0$, and no dyadic interval $[x, 2x)$ contains more than s elements of A . Then,*

$$|kA| \gg_k \frac{|A|^k}{s^k}$$

Proof. Without loss of generality, we may assume half the elements of A are nonnegative, else, replace A with $-A$ and repeat the proof since $|kA| = |k(-A)|$. Denote the nonnegative elements as $A' := \{a_1 < \dots < a_n\}$, and let

$$B := \{a_{2s}, a_{4s}, a_{6s}, \dots, a_{(2\lfloor \frac{n}{2s} \rfloor)s}\}.$$

Now, consider kB . Suppose

$$b_1 + \dots + b_k = b'_1 + \dots + b'_k. \quad (1)$$

for some $b_1 < \dots < b_k, b'_1 < \dots < b'_k \in B$. We claim that this implies $b_i = b'_i$ for all $i = 1, \dots, k$. Let $t \in \{1, \dots, k\}$ be the largest integer such that $b_t \neq b'_t$. Without loss of generality, if $b_t > b'_t$, then in fact $b_t > 2b'_t$ since they belong to nonconsecutive dyadic intervals. Moreover,

$$b'_1 + \dots + b'_{t-1} + b'_t \leq b'_t + b'_t < b_t < b_1 + \dots + b_t.$$

Hence, all the sums $b_1 + \dots + b_k$ are unique, and so

$$|kA| \geq |kB| = \binom{|B|}{k} \gg_k |B|^k \gg_k \frac{|A|^k}{s^k}.$$

□

Let $C \subseteq \mathbb{R}$. We call C_0, \dots, C_{k-1} a *decreasing partition* of C if

$$C = \bigcup_{i=0}^{k-1} C_i$$

and for any distinct $i, j \in \{0, \dots, k-1\}$, if $i < j$, then $|c| > |d|$ for all $c \in C_i, d \in C_j$.

Lemma 15. *Suppose that $C \subseteq \mathbb{R} - \{0\}$, and let*

$$1 = \delta_0 > \delta_1 > \dots > \delta_{k-1} > 0.$$

Moreover, suppose that C has the property that for any $c > d \in C$,

$$\frac{c}{d} - 1 > 2k \frac{\delta_i}{\delta_{i-1}}. \quad (2)$$

for all $i = 1, \dots, k-1$. Then for any decreasing partition C_0, \dots, C_{k-1} of C , then we must have that the sums

$$c_0\delta_0 + c_1\delta_1 + \dots + c_{k-1}\delta_{k-1}$$

are distinct for all $(c_0, c_1, \dots, c_{k-1}) \in C_0 \times C_1 \times \dots \times C_{k-1}$.

Proof. Suppose

$$\sum_{i=0}^{k-1} c_i \delta_i = \sum_{i=0}^{k-1} c'_i \delta_i \quad (3)$$

where $c_i, c'_i \in C_i$. Let j be the smallest integer in $\{0, \dots, k-1\}$ such that $c_j \neq c'_j$. Hence, we need only consider

$$\sum_{i=j}^{k-1} c_i \delta_i = \sum_{i=j}^{k-1} c'_i \delta_i \quad (4)$$

We will now derive a contradiction proving no such j exists and so (3) only holds when $c_i = c'_i$ for all i . For a contradiction, suppose $c_j > c'_j$. Dividing by $c'_j \delta_j$ on both sides and rearranging, the sum becomes

$$\frac{c_j}{c'_j} - 1 = \sum_{i=j+1}^{k-1} \frac{c'_i - c_i}{c'_j} \cdot \frac{\delta_i}{\delta_j}.$$

By (2), this implies that

$$\sum_{i=j+1}^{k-1} \frac{c'_i - c_i}{c'_j} \cdot \frac{\delta_i}{\delta_j} > 2k \frac{\delta_{j+1}}{\delta_j}.$$

On the other hand, since the C_i form a decreasing partition,

$$\left| \frac{c'_i - c_i}{c'_j} \right| < 2$$

for all $i \geq j+1$. Also, since $\delta_{j+1} > \delta_\ell > 0$ for all $\ell > j+1$

$$\frac{\delta_i}{\delta_j} < \frac{\delta_{j+1}}{\delta_j}.$$

So we get a contradiction since this would imply

$$\left| \sum_{i=j+1}^{k-1} \frac{c'_i - c_i}{c'_j} \cdot \frac{\delta_i}{\delta_j} \right| < 2k \frac{\delta_{j+1}}{\delta_j}.$$

□

3 Finding a Long Geometric Progression in A/A

The following two lemmas are variants of Lemma 2 in the work of Croot and Hart [5]. The first one is a repackaged version of the main idea in [6] which allows one to combinatorially find long progressions in difference (or quotient) sets. The second lemma builds upon the first by taking $(N+1)$ -tuples and showing that one can project them in a way that satisfies properties we will need later on.

Lemma 16. *For all $N \in \mathbb{N}$, $\epsilon > 0$, if $B \subseteq A \subseteq \mathbb{R}$ such that $|A \cdot A| < |A|^{1+\epsilon}$, then the following holds. There exists $\alpha \in \mathbb{R}$ and $\theta \in \frac{B}{B}$ such that there are $|A|^{N+2-7\epsilon N^2}$ tuples $(a, y_0, \dots, y_N) \in A^{N+2}$ such that*

$$ay_i \theta^i \in \alpha A$$

for all $i = 0, \dots, N$.

Proof. Let $\epsilon > 0$, and let $B \subseteq A \subseteq \mathbb{R}$ be such that $|A.A| < |A|^{1+\epsilon}$. Consider the following set:

$$E := \{(b_1, b_2, a_1, a_2, u, v, y_0, \dots, y_N, z_0, \dots, z_N) \in B^2 \times A^{2N+6} : va_1 b_1^i z_i = ua_2 b_2^i y_i \ i = 0, \dots, N\}.$$

For a vector $\mathbf{t} = (t_0, \dots, t_N) \in A^{(3)} \times A^{(4)} \dots \times A^{(N+3)}$, let

$$r(\mathbf{t}) := |\{(b, v, a, z_0, \dots, z_N) \in B \times A^{N+3} : vab^i z_i = t_i \text{ for } i = 0, \dots, N\}|.$$

Note that here is where we use the fact that $B \subseteq A$ in order to assume that $vab^i z_i \in A^{(i+3)}$. Now, one can use the Cauchy-Schwarz inequality to bound the size of E :

$$|E| = \sum_{\mathbf{t}} r(\mathbf{t})^2 \geq \frac{|B|^2 |A|^{2N+6}}{|A^{(3)}| |A^{(4)}| \dots |A^{(N+3)}|}$$

By the Plünnecke-Ruzsa inequality, since $|A| < |A|^{1+\epsilon}$, we then have that for all i , $|A^{(i)}| < |A|^{1+i\epsilon}$. Thus,

$$|E| \geq |B|^2 |A|^{N+5-\epsilon(3+4+\dots+N+3)} \geq |B|^2 |A|^{N+5-7\epsilon N^2}.$$

By the pigeonhole principle, there exists a $(b_1, b_2, u, v, a_1) \in B^2 \times A^3$ such that there are $|A|^{N+2-7\epsilon N^2}$ tuples $(a_2, y_0, \dots, y_N, z_0, \dots, z_N)$ such that for $i = 0, \dots, N$

$$va_1 b_1^i z_i = ua_2 b_2^i y_i.$$

Rearranging the above, we get that

$$z_i = a_2 \frac{u}{va_1} \left(\frac{b_2}{b_1} \right)^i y_i.$$

Letting $\alpha = \frac{va_1}{u}$ and $\theta = \frac{b_2}{b_1}$ proves the lemma. \square

Lemma 17. *Let $N, \ell \in \mathbb{N}$, $\epsilon > 0$ and let $c = 2\ell^{\lceil \log_2 N \rceil}$. There exists an $n_0 = n_0(N, \ell, \epsilon)$ such that if $A \subseteq \mathbb{R}$ is of size $n \geq n_0$ then the following holds. If $|A.A| \leq |A|^{1+\epsilon}$, then for any $B \subseteq A$ there exists $Y_0, \dots, Y_N \subseteq A$ such that*

$$1. |Y_i| \geq |A|^{1-O(\epsilon c N^4)}.$$

2. *For any collection of subsets $Y'_i \subseteq Y_i$ satisfying $|Y'_i| \leq c$ then there exists an $\alpha \in \mathbb{R}$, $\theta \in \frac{B}{B}$, and an $A' \subseteq A$ of size at least $\sqrt{|A|}$ such that*

$$ay_i \theta^i \in \alpha A$$

for all $a \in A'$, $y_i \in Y'_i$, $i \in \{0, \dots, N\}$.

We first need a graph theoretic lemma. It is a slight variant of a lemma found in the excellent survey by Fox and Sudakov about the technique of dependent random choice [10]. For a graph G and $T \subseteq G$, let $\Gamma(T)$ denote the set of common neighbors of T ; that is, the set of all vertices adjacent to every vertex in T .

Lemma 18. *Let $a, m, r \in \mathbb{N}$. Let $G = [X, Y]$ be a bipartite graph with $|E(G)|$ edges. If there exists a $t \in \mathbb{N}$ such that*

$$\frac{|E(G)|^t}{|X|^t |Y|^{t-1}} - \binom{|Y|}{r} \left(\frac{m}{|X|} \right)^t \geq a$$

then there exists a set of vertices in Y of size a such that every r of them have at least m common neighbors.

Proof. Let $T \subseteq X$ be a set of t vertices chosen uniformly at random with repetition. Let $\Gamma(T)$ denote the set of common neighbors of T , and let $Z = |\Gamma(T)|$. Then, by linearity of expectation and Hölder's inequality

$$\mathbb{E}(Z) = \sum_{y \in Y} \mathbb{P}(T \subseteq N(y)) = \sum_{y \in Y} \left(\frac{|N(y)|}{|X|} \right)^t \geq \frac{|E(G)|^t}{|X|^t |Y|^{t-1}}.$$

Now, let W be the random variable associated to the number of sets of r vertices in $\Gamma(T)$ with less than m common neighbors. We want W to be small so that we may modify all these deficient sets and prove the lemma. First, note that for any set $S \subseteq Y$ of size r with less than m common neighbors, the probability that S is also a subset of $\Gamma(T)$ is

$$\left(\frac{|\Gamma(S)|}{|X|} \right)^t$$

since the only way that $S \subseteq \Gamma(T)$ is if every vertex from the common neighborhood of S gets chosen in T . Hence,

$$\mathbb{E}(W) \leq \left(\frac{|\Gamma(S)|}{|X|} \right)^t \binom{|Y|}{r} < \frac{m^t}{|X|^t} \binom{|Y|}{r}.$$

Therefore, there exists a choice of T such that

$$\mathbb{E}(Z - W) > \frac{|E(G)|^t}{|X|^t |Y|^{t-1}} - \binom{|Y|}{r} \left(\frac{m}{|X|} \right)^t \geq a.$$

Let T be chosen such that the above holds. For each set $S \subseteq \Gamma(T)$ of size r with less than m common neighbors, remove a vertex arbitrarily from S . After this process, $\Gamma(T)$ still has at least a vertices left, and every set of size r has at least m common neighbors. \square

Proof of Lemma 17. Apply Lemma 16 to get an $\alpha \in \mathbb{R}$ and a $b_1 > b_2 \in B$ such that there are $|A|^{N+2-7\epsilon N^2}$ tuples

$$T := (a, y_0, \dots, y_N) \in A^{N+2}$$

such that

$$\alpha a y_i \theta^i \in A \text{ for } i = 0, \dots, N. \quad (5)$$

Let $G[X, Y]$ be the bipartite graph defined by $X = A$, $Y = A^{N+1}$, and edges defined by the set T . Observe that for any constant r depending only on ℓ and N there exists a t and an ϵ such that if A is sufficiently large, then

$$\frac{|A|^{t(N+2-7\epsilon N^2)}}{|A|^t |A|^{(t-1)(N+1)}} - \binom{|A|^{N+1}}{r} \left(\frac{|A|^{t/2}}{|A|^t} \right) \geq |A|^{N+1-7\epsilon t N^2} - |A|^{r(N+1)-t/2} \geq \frac{1}{2} |A|^{N+1-7\epsilon t N^2}.$$

In particular, one may choose $t = 2r(N+1)$. Hence, we may apply Lemma 18 with $a = \frac{1}{2} |A|^{N+1-14\epsilon r N^3}$, $m = |A|^{1/2}$, and $r = c(N+1)$. Let $Y' \subseteq Y$ denote the set found by Lemma 18 with the specified property.

Each vertex $v \in Y'$ is associated to a corresponding $(N+1)$ -tuple; for $i = 0, \dots, N$, let Y_i be the projection of Y' onto the i th coordinate axis. One can see that $|Y_i| \geq |A|^{1-O(\epsilon c N^4)}$. Consider an arbitrary collection of subsets $Y'_i \subseteq Y_i$ satisfying $|Y'_i| \leq c$. Let $y_{i,j} \in Y'_i$. Our goal is to show there is a fixed set $A' \subseteq A$ of $|A|^{1/2}$ elements such that (5) holds for all $y_{i,j}$, $a \in A'$, $i = \{0, \dots, N\}$.

Since $y_{i,j} \in Y'_i \subseteq Y_i$, there exists a corresponding $(N+1)$ -tuple

$$(u_0, u_1, \dots, u_{i-1}, y_{i,j}, u_{i+1}, \dots, u_N) \in Y'.$$

For each $y_{i,j}$, arbitrarily choose such a tuple in Y' , and denote the tuple as $v_{i,j}$. Let V be the collection of all such $v_{i,j}$. So, letting $|V| \leq c(N+1)$ be the constant r in the application of Lemma 18, we can conclude that there is a set of $|A|^{1/2}$ vertices in X adjacent to every vertex in V . Let A' be this set of $|A|^{1/2}$ vertices. Hence, there is a set of $|A|^{1/2}$ elements such that for any $y_{i,j} \in Y'_i$ (5) holds for all $a \in A'$, $i \in \{0, \dots, N\}$. \square

4 Intersections of Multifold Sumsets

We now prove the following lemma that gives us information when lots of multifold sumsets intersect trivially. This lemma is what introduces a significant amount of loss in the strength of our overall bound in Theorem 1 – that is, it is the main obstruction in improving the exponent $\exp(c\sqrt{\log h})$ to some fixed power of h .

Lemma 19. *Let $A \subseteq \mathbb{R}$ be of size n and $\ell, t \in \mathbb{N}$. Let $A_i \subseteq A$ for $i = 1, \dots, 2^t$ be such that*

$$\bigcap_{i=1}^{2^t} f(t, i) \ell^{g(t, i)} A_i - f(t, i) \ell^{g(t, i)} A_i = \{0\}.$$

Then, there exists an $i \in \{2, \dots, t+1\}$ and an $j \in \{1, \dots, 2^t\}$ such that

$$|(\ell^{i-1} + \ell^i)A| \geq n^{\frac{1}{3^{t+1}}} |\ell^i A_i|.$$

The functions f and g in the above lemma are defined as follows. For $a \in \mathbb{N}$, $b = 1, \dots, 2^a$, define $f(a, b)$ recursively as follows:

$$\begin{aligned} f(1, 1) &:= 1, f(1, 2) := 2, \\ f(a, 2b-1) &:= f(a-1, b); b = 1, \dots, 2^{a-1} \end{aligned} \tag{6}$$

$$f(a, 2b) := 2f(a, 2b-1) = 2f(a-1, b); b = 1, \dots, 2^{a-1} \tag{7}$$

For the benefit of the reader, we list the first few values of $f(a, b)$:

$$\begin{aligned} f(1, 1) &= 1; f(1, 2) = 2 \\ f(2, 1) &= 1; f(2, 2) = 2; f(2, 3) = 2; f(2, 4) = 4 \\ f(3, 1) &= 1; f(3, 2) = 2; f(3, 3) = 2; f(3, 4) = 4; f(3, 5) = 2; f(3, 6) = 4; f(3, 7) = 4; f(3, 8) = 8 \end{aligned}$$

Observe that

$$f(a, b) = 2^k \text{ for some } k \leq a. \tag{8}$$

Denote $g(a, b) := \log_2 f(a, b) + 1$. Observe that by (7),

$$g(a, 2b) = g(a, 2b-1) + 1 \tag{9}$$

and by (8),

$$g(a, b) \leq a + 1. \tag{10}$$

The following covering lemma, which is potentially of independent interest, is the main tool in proving Lemma 19.

Lemma 20. *For any X, Y in an abelian group G and any $K \in \mathbb{N}$, there exists an $X' \subseteq X$ such that either*

1. $|X'| \geq K$ and $X' - X' \cap Y - Y = \{0\}$, or
2. $|X'| \geq \frac{|X|}{K}$ and $X' - X' \subseteq 2Y - 2Y$.

This follows quickly from the following graph theory lemma.

Lemma 21. *For any graph G and any $0 \leq K \leq |G|$, G contains an independent set of size at least K or a vertex of degree at least $|G|/K$.*

Proof. If G has a vertex of degree at least $|G|/K$, we are done. Hence, the maximum degree of G , $\Delta(G)$ is less than $|G|/K$. By the greedy algorithm, we can find an independent set of size

$$K \geq \left\lfloor \frac{|G| + \Delta}{\Delta + 1} \right\rfloor.$$

□

Proof of Lemma 20. Let $G = (V, E)$ be the graph defined by $V(G) := X$ and $\{u, v\} \in E(G)$ if $u - v \in Y - Y$. Observe that since $Y - Y$ is symmetric, these edges are undirected. If G contains an independent set X' of size at least K , for any distinct $u, v \in X'$, $u - v \notin Y - Y$. Hence, $X' - X' \cap Y - Y = \{0\}$. Otherwise, G contains a vertex, a , of degree at least $\frac{|X|}{K}$. Letting the neighborhood of this vertex be X' , for any $u, v \in X'$, $\{u, a\}$ and $\{a, v\}$ are edges. Since $u - v = u - a + a - v$, we have that $u - v \in 2Y - 2Y$. □

Proof of Lemma 19. We perform the following algorithm to find such an i, j as in the conclusion of the lemma. We outline steps $j = 0, \dots, t - 2$.

Step 0: Let $A_{0,i} := \ell^{g(t,i)} A_i$. For $i = 1, \dots, 2^{t-1}$, apply Lemma 20 with

$$X := A_{0,2i-1}, Y := A_{0,2i}, \text{ and } K := K_0 = n^{\frac{1}{3^t}},$$

and observe which case holds. If for any i , Case 1 holds, we halt since this implies that there exists an $X' \subseteq X$ with $|X'| \geq n^{\frac{1}{3^t}}$ and

$$|(\ell^{g(t,2i-1)} + \ell^{g(t,2i)})A| \geq |A_{0,2i-1} + A_{0,2i}| \geq |X' + Y| = |X'||Y| \geq n^{\frac{1}{3^t}} |\ell^{g(t,2i)} A_{2i}|.$$

This satisfies the conclusion of the lemma with $k = g(t, 2i)$ and $j = 2i$. Hence, we may assume Case 2 holds for all i . Therefore, there exists an $X' \subseteq X$ such that $X' - X' \subseteq 2Y - 2Y$. Adding $X' - X'$ to itself multiple times also implies for any positive integer s , $sX' - sX' \subseteq 2sY - 2sY$. In particular for $s = f(t, 2i - 1)$,

$$\begin{aligned} f(t, 2i - 1)X' - f(t, 2i - 1)X' &\subseteq 2f(t, 2i - 1)Y - 2f(t, 2i - 1)Y \\ &= 2f(t, 2i - 1)A_{0,2i} - 2f(t, 2i - 1)A_{0,2i} \\ &= f(t, 2i)A_{0,2i} - f(t, 2i)A_{0,2i}. \end{aligned} \tag{11}$$

where we used (7) in the last equality. Also,

$$\begin{aligned} f(t, 2i - 1)X' - f(t, 2i - 1)X' &\subseteq f(t, 2i - 1)X - f(t, 2i - 1)X \\ &= f(t, 2i - 1)A_{0,2i-1} - f(t, 2i - 1)A_{0,2i-1} \end{aligned} \tag{12}$$

Letting $A_{1,i} := X'$, we then have that by (6), (11), and (12)

$$\begin{aligned} \bigcap_{i=1}^{2^{t-1}} f(t-1, i)A_{1,i} - f(t-1, i)A_i &\subseteq \bigcap_{i=1}^{2^t} f(t, i)A_{0,i} - f(t, i)A_{0,i} \\ &= \bigcap_{i=1}^{2^t} f(t, i)\ell^{g(t,i)}A_i - f(t, i)\ell^{g(t,i)}A_i = \{0\}. \end{aligned}$$

And we also have that

$$|A_{1,i}| \geq \frac{|A_{0,2i-1}|}{K_0}$$

The next steps, Steps $j = 1, \dots, t-2$, are iterations of this argument with a very slight change in the choice of X and Y in the application of Lemma 20.

Step j: Let $A_{j,i} \subseteq A_{j-1,2i-1}$ be as specified in Step (j-1) of the algorithm. In particular, $A_{j,i}$ satisfies

$$|A_{j,i}| \geq \frac{|A_{j-1,2i-1}|}{K_{j-1}}.$$

An easy inductive argument shows that there exists an s such that

$$A_{j,i} \subseteq A_{j-1,2i-1} \subseteq \dots \subseteq A_{0,s} \subseteq \ell^{g(t-j,i)}A_s. \quad (13)$$

where we draw the reader's attention to the fact that the subscript $A_{j,i}$ determines the exponent at the end, $g(t-j, i)$. For $i = 1, \dots, 2^{t-j-1}$, apply Lemma 20 with $X = A_{j,2i-1}$, $Y = A_{j,2i}$, $K := K_j = n^{\frac{1}{3^{t-j}}}$, and observe which case holds. If for any i , Case 1 holds, we halt since by Lemma 11 this implies that

$$\begin{aligned} |X' + Y| &= |X'| |Y| \geq K_j |A_{j,2i}| \\ &\geq \frac{K_j}{K_{j-1}} |A_{j-1,4i-1}| \\ &\vdots \\ &\geq \frac{K_j}{K_{j-1}K_{j-2}\dots K_0} |A_{0,s}| \\ &= n^{\frac{1}{3^{t+1}}} |\ell^{g(t-j,2i)}A_s| \end{aligned} \quad (14)$$

for some integer s . On the other hand, using (13) and (9), we have

$$\begin{aligned} |X' + Y| &\leq |X + Y| = |A_{j,2i-1} + A_{j,2i}| \\ &\leq |A_{j-1,4i-3} + A_{j-1,4i-1}| \\ &\vdots \\ &\leq |A_{0,s_1} + A_{0,s}| \leq |(\ell^j + \ell^{j+1})A| \end{aligned} \quad (15)$$

for $j = g(t-j, 2i-1)$. Combining (14) and (15) shows that we have satisfied the conclusion of the Lemma.

Hence, we may assume Case 2 holds for all i . Therefore, there exists an $X' \subseteq X$ with $|X'| \geq |X|/K_j$ such that $X' - X' \subseteq 2Y - 2Y$. Moreover, for any positive integer s , $sX' - sX' \subseteq 2sY - 2sY$.

For $s = f(t - j - 1, i)$

$$\begin{aligned} f(t - j - 1, i)X' - f(t - j - 1, i)X' &\subseteq 2f(t - j - 1, i)Y - 2f(t - j - 1, i)Y \\ &= 2f(t - j - 1, i)A_{j,2i} - 2f(t - j - 1, i)A_{j,2i} \\ &= f(t - j, 2i)A_{j,2i} - f(t - j, 2i)A_{j,2i}. \end{aligned} \quad (16)$$

where we used (6) in the last equality. Also,

$$\begin{aligned} f(t - j - 1, i)X' - f(t - j - 1, i)X' &\subseteq f(t - j - 1, i)X - f(t - j - 1, i)X \\ &= f(t - j, 2i - 1)A_{j,2i-1} - f(t - j, 2i - 1)A_{j,2i-1} \end{aligned} \quad (17)$$

Letting $A_{j+1,i} := X'$, we then have that by (7), (16), and (17)

$$\bigcap_{i=1}^{2^{t-j-1}} f(t - j - 1, i)A_{j+1,i} - f(t - j - 1, i)A_{j+1,i} \subseteq \bigcap_{i=1}^{2^{t-j}} f(t - j, i)A_i - f(t - j, i)A_i = \{0\}.$$

We now proceed to Step $j+1$ with $A_{j+1,i}$, $i = 1, \dots, t - j - 1$.

Step $t - 1$: If we have not halted, then at this point, we only have 2 sets, $A_{t-1,1}, A_{t-1,2}$, such that

$$f(1, 1)A_{t-1,1} - f(1, 1)A_{t-1,1} \cap f(1, 2)A_{t-1,2} - f(1, 2)A_{t-1,2} = \{0\}.$$

Since $f(1, 1) = 1$, $f(1, 2) = 2$, and

$$A_{t-1,1} - A_{t-1,1} \cap A_{t-1,2} - A_{t-1,2} \subseteq A_{t-1,1} - A_{t-1,1} \cap 2A_{t-1,2} - 2A_{t-1,2} = \{0\}$$

we then have by Lemma 11

$$|A_{t-1,1} + A_{t-1,2}| = |A_{t-1,1}||A_{t-1,2}|.$$

Tracing back our steps in the algorithms as we did in (14) and (15), we get that

$$\begin{aligned} |A_{t-1,1}||A_{t-1,2}| &\geq \frac{|A_{t-2,1}||A_{t-2,3}|}{K_{t-1}^2} \geq \frac{|A_{t-3,1}||A_{t-3,5}|}{K_{t-1}^2 K_{t-2}^2} \\ &\geq \frac{|A_{t-3,1}||A_{t-3,9}|}{K_{t-1}^2 K_{t-2}^2 K_{t-3}^2} \\ &\vdots \\ &\geq \frac{|A_{0,1}||A_{0,2^{t-1}+1}|}{K_{t-1}^2 K_{t-2}^2 K_{t-3}^2 \dots K_0^2} \geq n^{\frac{1}{3^{t+1}}} |\ell^2 A_{2^{t-1}+1}| \end{aligned} \quad (18)$$

Note that we used the fact that $|A_{1,0}| \geq n$ in the last inequality. On the other hand,

$$\begin{aligned} |A_{t-1,1} + A_{t-1,2}| &\leq |A_{t-2,1} + A_{t-2,3}| \leq |A_{t-3,1} + A_{t-3,5}| \\ &\vdots \\ &\leq |A_{0,1} + A_{0,2^{t-1}+1}| \\ &\leq |\ell A_1 + \ell^2 A_{2^{t-1}+1}| \leq |(\ell + \ell^2)A| \end{aligned} \quad (19)$$

Combining (18) and (19) completes the proof of the lemma. \square

5 Proof of Main Theorem

The proof of our main theorem is iterative. The argument splits into two cases: in one case, we prove our bound directly similar to [5]; the other case we have to iteratively use Lemma 19 to get a small amount of growth each iteration while passing to subsets of our original set. After enough iterations, we prove our bound.

Proposition 22. *Let $h \in \mathbb{N}$. Let*

$$e^{\sqrt{\frac{1}{100} \log \frac{h}{2}}} \text{ and } \ell := k^8.$$

There exists an $\epsilon' := \epsilon'(h)$ such that for any $0 < \epsilon < \epsilon'$ there exists an $n_0 := n_0(\epsilon, h)$ such that if $A \subseteq \mathbb{R}$ is of size $n \geq n_0$ and $|A.A| \leq |A|^{1+\epsilon}$, then either

$$|hA| \geq |A|^{\Omega(k)}$$

or there exists an $A' \subseteq A$ and a $c := c(h)$ such that $|A'| \geq |A|^{1-c\epsilon}$, and

$$|(\ell^j + \ell^{j-1})A| \gg_h |A|^{\frac{1}{22k^6}} |\ell^j A'|$$

for some $j \in \{2, \dots, \log 8k^5\}$.

Proof of Proposition 22. Let $A \subseteq \mathbb{R}$ be such that $|A.A| \leq |A|^{1+\epsilon}$. Let k, ℓ be constants depending on h as specified in the statement of the proposition. Apply Corollary 13 to get a set of polynomials $f_j(x)$ for $j = 2, \dots, k-1$ such that each polynomial has coefficients in $\{-1, 0, 1\}$, $f_j(x)$ has a root at $x = 1$ of order exactly j , and $f_j(x)$ has at most $j^2 \leq k^2$ nonzero terms. Let $f_0(x) := 1$, and $f_1(x) := x - 1$.

$$N := \max_j \{\deg(f_j) : j = 0, \dots, k-1\}$$

and let $S \subseteq \{0, \dots, N\}$ be such that $i \in S$ if and only if there is an $f_j(x)$ such that the coefficient of x^i is nonzero. Let $M := |S|$ and observe that $M \leq k^3$.

Denote $A := \{a_1 < \dots < a_n\}$, let $0 < \delta < 1/4$ be a parameter chosen later, and let $s := \lfloor n^\delta \rfloor$. Let

$$B' := \{a_i, a_{i+1}, \dots, a_{i+s-1}\}$$

be chosen such that a_{i+s-1}/a_i is minimal. By Lemma 14, if no dyadic interval contains more than s elements of A , we are done. Hence, $B' \subseteq [x, 2x)$ for some $x \in \mathbb{R}$. Let $0 < \gamma < 1$ be a small constant depending on h to be chosen later. There exists a subinterval

$$[y, y + \gamma x) \subseteq [x, 2x)$$

with at least γs elements of A in it. Let B be the intersection of A with this subinterval. So $B \subseteq A$ has the properties that $|B| \geq \gamma s$ and for any $b, b' \in B$,

$$\left| \frac{b}{b'} - 1 \right| < \gamma.$$

The latter property will be important when we later consider polynomials with roots at 1 evaluated at $\frac{b}{b'}$.

Apply Lemma 17 with N, ℓ, ϵ, B to find a set of $Y_i \subseteq A$, $\alpha \in \mathbb{R}$, $\theta \in B/B$, satisfying the conclusion of the lemma. We will discard some of the sets from Y_0, \dots, Y_N in the following way. If

$i \notin S$, then we throw out Y_i . Abusing our notation, relabel the remaining sets as Y_1, \dots, Y_M . Let $t = \lceil \log_2 M \rceil \leq \lceil \log_2 k^3 \rceil$. If

$$\bigcap_{i=1}^M \ell^t Y_i - \ell^t Y_i = \{0\}$$

then we may apply Lemma 19 to conclude that there exists an $i \in \{2, \dots, t+1\}$ and a $j \in \{1, \dots, 2^t\}$ such that

$$|(\ell^{i-1} + \ell^i)A| \geq |A|^{\frac{1}{3^{t+1}}} |\ell^i Y_i| \geq |A|^{\frac{1}{22k^6}} |\ell^i Y_i|.$$

This satisfies the second conclusion of the proposition, so we may assume that there exists a nonzero β in the above intersection. That is, a nonzero β such that for $i = 1, \dots, M$,

$$\beta = \sum_{j=1}^{\ell^t} y_{i,j} - \sum_{j=\ell^t+1}^{2\ell^t} y_{i,j}$$

where $y_{i,j} \in Y_i$. Letting $Y'_i := \{y_{i,j} : j = 1, \dots, 2\ell^t\}$, by the conclusion of Lemma 17, there exists an $A' \subseteq A$ of size at least $|A|^{1/2}$ such that

$$ay_{i,j}\theta^i \in \alpha A \text{ for } i = 1, \dots, M, \text{ and any } a \in A'. \quad (20)$$

Denote $A' := \{a_1 < a_2 < \dots < a_{|A'|}\}$, and let $C := \{a_{i_1}, a_{i_2}, \dots, a_{i_r}\}$ where

$$i_j = j \lfloor n^{1/4} \rfloor \text{ and } r = \left\lfloor \frac{|A'|}{n^{1/4}} \right\rfloor.$$

This ensures that we have

$$\frac{c}{c'} > \theta \text{ for any } c, c' \in C \quad (21)$$

by our choice of B' along with the fact that $s < \lfloor n^{1/4} \rfloor$. Decompose C into C_0, C_1, \dots, C_{k-1} where all elements of C_i are greater than all elements of C_j for $i < j$, and for all $i = 0, \dots, k-2$, $|C_i| = \lfloor |C|/k \rfloor$. For $i = 0, \dots, k-1$, let $\delta_i := f_i(\theta)$. Now consider sums of the form

$$\Sigma = \{\beta(c_0\delta_0 + c_1\delta_1 + \dots + c_{k-1}\delta_{k-1}) : c_i \in C_i\}. \quad (22)$$

We verify that C and δ_i satisfy the requirements of Lemma 15 as follows. Since

$$\frac{\delta_i}{\delta_{i-1}} = \frac{f_i(x)}{f_{i-1}(x)} = (x-1)g_i(x)$$

where the coefficients of g_i depend only on k , we may choose γ small enough such that

$$\theta - 1 < \frac{1}{g_i(\theta)}.$$

So we have that $\delta_{i-1} > \delta_i$ for all $i = 1, \dots, k-1$. Let $c, d \in C$. From (21), we have that $\frac{c}{d} > \theta$. However, by choosing δ small enough, we can assume that in fact $\frac{c}{d} > \theta^r$ for any $r = r(k)$. Hence,

$$\frac{c}{d} - 1 > \theta^r - 1 = (\theta - 1)(1 + \theta + \dots + \theta^{r-1}) \geq (\theta - 1)r.$$

By choosing $r > 2k \cdot g_i(\theta)$, we have

$$\frac{c}{d} - 1 \geq (\theta - 1)2k \cdot g_i(\theta) = 2k \frac{\delta_i}{\delta_{i-1}}.$$

So by Lemma 15, all the sums of the form (22) are distinct, and so

$$|\Sigma| \geq \prod_{i=0}^{k-1} |C_i|.$$

We can rewrite (22) by grouping like powers of θ as

$$\beta \left[\left(\sum_{i=0}^{k-1} \epsilon_{0,i} c_i \right) \theta^0 + \left(\sum_{i=0}^{k-1} \epsilon_{1,i} c_i \right) \theta^1 + \dots + \left(\sum_{i=0}^{k-1} \epsilon_{M,i} c_i \right) \theta^N \right]$$

where $\epsilon_{i,j} \in \{-1, 0, 1\}$. Recall that S is the set of powers of θ that have at least one nonzero coefficient in some polynomial f_j . Denoting S as $i_1 < i_2 < \dots < i_M$, we can rewrite the above as

$$\beta \left[\left(\sum_{i=0}^{k-1} \epsilon_{i_1,i} c_i \right) \theta^{i_1} + \left(\sum_{i=0}^{k-1} \epsilon_{i_2,i} c_i \right) \theta^{i_2} + \dots + \left(\sum_{i=0}^{k-1} \epsilon_{i_M,i} c_i \right) \theta^{i_M} \right].$$

Distribute β to each summand, and expand it uniquely for each power of θ to get

$$= \sum_{j=0}^{k-1} \sum_{i=1}^{\ell^t} \epsilon_{i_1,j} c_j (y_{1,i} - y_{1,\ell^t+i}) \theta^{i_1} + \dots + \sum_{j=0}^{k-1} \sum_{i=1}^{\ell^t} \epsilon_{i_M,j} c_j (y_{M,i} - y_{M,\ell^t+i}) \theta^{i_M} \quad (23)$$

Since our choices of θ and $y_{i,j}$ satisfy (20), we have that each element in this sum is in $\pm \alpha * A$. Hence, we have that for ℓ_1, ℓ_2 large enough,

$$|\ell_1(\alpha * A) - \ell_2(\alpha * A)| = |\ell_1 A - \ell_2 A| \geq \prod_{i=0}^{k-1} |C_i| \geq \left\lfloor \frac{|C|}{k} \right\rfloor^{k-1} \gg_k |A|^{\frac{k-1}{4}}.$$

Recall that $\ell = k^8$, $M \leq k^3$, and $t = \lceil \log_2 M \rceil \leq \log_2 2k^3 \leq \log_e 3k^5$. So, we have $M \cdot 2\ell^t$ nonzero terms in $\sigma \in \Sigma$. We bound this as

$$M \cdot 2\ell^t \leq 2k^3 k^{8 \log_e 3k^5} = 2k^{100 \log k}$$

So, choosing $k := e^{\sqrt{\frac{1}{100} \log \frac{h}{2}}}$ proves our theorem:

$$|hA| \geq \sqrt{|hA - hA|} \geq |A|^{\Omega(e^{\sqrt{\frac{1}{100} \log h}})}$$

□

5.1 The Iterative Case

We are now able to prove Theorem 1.

Proof of Theorem 1. We iteratively apply Proposition 22 in the following algorithm.

Step 0: Let k and ℓ be functions of h as specified in the statement of Proposition 22, and let $0 < \epsilon < \epsilon'$ where ϵ' is some unspecified function of h taken to be sufficiently small. Let $\ell_0 := \ell$, $A_0 := A$, and $\epsilon_0 := \epsilon$. Since $|A_0 \cdot A_0| \leq |A_0|^{1+\epsilon_0}$, we may apply Proposition 22 to A_0 . If $|hA_0| \geq |A_0|^{\Omega(k)}$, then we are done. Else, there exists a $j \in \{2, \dots, \log 8k^5\}$ and an $A'_0 \subseteq A_0$ such that

$$|(\ell^j + \ell^{j-1})A_0| \gg_h |A_0|^{\frac{1}{22k^6}} |\ell^j A'_0| \text{ and } |A'_0| \geq |A_0|^{1-c\epsilon}$$

where c is a constant depending on h . Let $A_1 := A'_0$ and continue to Step 1.

For $j = 1, \dots, \frac{1}{2}\ell$, we do the following.

Step j: Let A_j be as specified in the previous step. Since

$$|A_j \cdot A_j| \leq |A_{j-1} \cdot A_{j-1}| \leq |A_{j-1}|^{1+\epsilon_{j-1}} \leq |A_j|^{\frac{1+\epsilon_{j-1}}{1-\epsilon_{j-1}}} \leq |A_j|^{1+2c\epsilon_{j-1}}$$

where we assumed ϵ_{j-1} is sufficiently small in the last inequality. Let $\epsilon_j := 2c\epsilon_{j-1}$. Let $\ell_j := \ell - j$. This determines h_j and k_j as

$$h_j = e^{\frac{25}{36}(\log(\ell-j))^2} ; k_j = (k^8 - j)^{1/8}.$$

Applying Proposition 22 to A_j with and h_j , we get that either

$$|hA| \geq |h_j A_j| \geq |A_j|^{\Omega(k_j)} \geq |A_j|^{\Omega((k^8-j)^{1/8})} = |A_j|^{\Omega(k)} \geq |A|^{(1-(2c)^j)\epsilon} = |A|^{\Omega(k)}$$

which proves the theorem for ϵ sufficiently small – so we exit the algorithm. Or, there exists an $A'_j \subseteq A_j$ of size $|A'_j| \geq |A_j|^{1-\epsilon_j}$ and a $t_j \in \{2, \dots, \log 8k^5\}$ such that

$$|(\ell_j^{t_j} + \ell_j^{t_j-1})A_j| \geq |A_j|^{\frac{1}{22k^6}} |\ell_j^{t_j} A'_j| \geq |A_j|^{\frac{1}{22k^6}} |\ell_j^{t_j} A'_j| \geq n^{\frac{1}{23k^6}} |\ell_j^{t_j} A'_j|$$

where we used the fact that ϵ is sufficiently small and n is sufficiently large depending on h in the last inequality. Letting $A_{j+1} := A'_j$ we continue to Step $j+1$.

Analysis of Algorithm: Since $\ell_j = \ell - j$, and we perform at most $\ell/2$ steps, $\ell_j \geq \ell/2$. Assume the algorithm runs and finishes Step $\ell/2$. Each step in the algorithm produces a $t_j \in \{2, \dots, \log 8k^5\}$. By averaging, there is some integer $s \in \{2, \dots, \log 8k^5\}$ that appears in the algorithm at least $\frac{\ell}{2 \log 8k^5}$ times. Denote j_1, \dots, j_q as the steps in which s is chosen. It is easy to verify that by the definition of ℓ_j ,

$$\ell_j^2 + \ell_j \leq \ell_{j-1}^2,$$

and so we must also have that

$$\ell_j^s + \ell_j^{s-1} \leq \ell_{j-1}^2 \cdot \ell_j^{s-2} \leq \ell_{j-1}^s.$$

So,

$$\begin{aligned} |(\ell_{j_1}^s + \ell_{j_1}^{s-1})A_{j_1}| &\geq n^{\frac{1}{23k^6}} |\ell_{j_1}^s A'_{j_1}| \geq \\ &\geq n^{\frac{1}{23k^6}} |(\ell_{j_2}^s + \ell_{j_2}^{s-1})A_{j_2}| \geq n^{\frac{2}{23k^6}} |\ell_{j_2}^s A'_{j_2}| \geq \\ &\vdots \\ &\geq n^{\frac{q}{23k^6}} |(\ell_{j_q}^s + \ell_{j_q}^{s-1})A_{j_q}| \geq n^{\frac{\ell}{2 \log 8k^5} \cdot \frac{1}{23k^6}} = n^{\Omega(k)} \end{aligned}$$

where we used the fact that $q \geq \frac{\ell}{2 \log 8k^5}$ and $\ell = k^8$ in the last inequality. Since

$$\ell_{j_1}^s \leq \ell^{\log 8k^5} \leq k^{8(\log 8k^5)} \leq k^{100 \log k} = h$$

we have that

$$|hA|^2 \geq |(\ell_{j_1}^s + \ell_{j_1}^{s-1})A_{j_1}| \geq n^{\Omega(k)}$$

proving our theorem. \square

The authors thank Jacob Fox for simplifying the original statement and proof of Lemma 20.

References

- [1] J. Bourgain and M-C. Chang. On the size of the k -fold sum and product sets of integers. *J. Amer. Math. Soc.* **17.2** (2003), 473-497.
- [2] M-C. Chang. The Erdős-Szemerédi problem on sum set and product set. *Annals of Math.* **157** (2003), 939-957.
- [3] M-C. Chang. Sum and product of different sets. *Contributions to Discrete Math.* **50** (2006), 57-67.
- [4] Y-G. Chen. On sums and products of integers. *Proc. Amer. Math. Soc.* **127.7** (1999), 1927-1933.
- [5] E. Croot and D. Hart. h -fold sums from a set with few products. *SIAM J. of Discrete Math.* **24** (2010), 505-519.
- [6] E. Croot, I. Z. Ruzsa, T. Schoen. Arithmetic progressions in sparse sumsets. *INTEGERS*. **7(2)** (2007), #A10.
- [7] P. Erdős and E. Szemerédi. On sums and products of integers. *Studies in Pure Mathematics, To the Memory of Paul Turán* (1983), Birkhauser Verlag, Basel. 213-218.
- [8] G. Elekes. On the number of sums and products. *Acta Arith.* **81** (1997), 365-367.
- [9] K. Ford. Sums and products from a finite site of real numbers. *Ramanujan J.* **2** (1998), 59-66.
- [10] J. Fox and B. Sudakov. Dependent random choice. *Random Structures and Algorithms*. **38** (2011), 68-99.
- [11] S. Konyagin. Personal communication.
- [12] L. Li. Multi-fold sums from a set with few products. *arXiv:1106.6074v1*, (2011).
- [13] M. Nathanson. On sums and products of integers. *Proc. Amer. Math. Soc.* **125.1** (1997), 9-16.
- [14] I. Z. Ruzsa. An application of graph theory to additive number theory. *Scientia, Ser. A.* **3** (1989), 97-109.
- [15] J. Solymosi. On the number of sums and products. *Bull. Lon. Math. Soc.* **37** (2005), 491-494.
- [16] J. Solymosi. Bounding multiplicative energy by the sumset. *Advances in Math.* **222.2** (2009), 402-408.
- [17] T. Tao and V. Vu. Additive Combinatorics. *Cambridge University Press*. (2010).
- [18] T. Wooley. Multigrade efficient congruencing and Vinogradov's mean value theorem. *arXiv:1310.8447*, (2013).